

UNITED STATES DISTRICT COURT

for the
Northern District of Texas

FILED

DEC 18 2015

CLERK, U.S. DISTRICT COURT

By Deputy

Case No. 4:15-MJ-560

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

One homebuilt desktop computer and devices seized
from J. Pavilik's residence located at FBI Field Office
1 Justice Way, Dallas, Texas

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

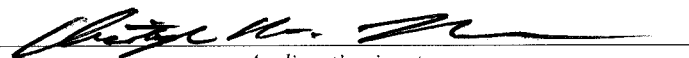
18 U.S.C. § 2252A

Possession and/or Access with Intent to
View Child Pornography

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Christopher W. Thompson, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/18/2015

City and state: Fort Worth, Texas


Judge's signature

United States Magistrate Judge Jeffrey L. Cureton

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Christopher W. Thompson, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the FBI since April 2004, and I am currently assigned to the Dallas Division, which is located at One Justice Way, Dallas, Texas 75220. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am currently assigned to a Child Exploitation Task Force, wherein my duties and responsibilities include investigating criminal violations relating to the sexual exploitation of children. I have investigated these violations since 2004 and have gained expertise in these types of investigations through training in seminars, classes, and my everyday work. In addition, I have received specialized training in the investigation and enforcement of federal child pornography laws, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. §2256) in all forms of media, including computer media.

2. This affidavit is submitted in support of an application for a warrant to search multiple digital devices, including a homebuilt desktop computer bearing a label MS-7309 (the SUBJECT COMPUTER), as further described in Attachment A, which is incorporated herein by reference.

Located within the items to be searched, I seek to seize evidence and instrumentalities of criminal violations, which relate to the knowing receipt and possession of child pornography. I request authority to search the SUBJECT DEVICES and other evidence, for the items specified in Attachment B (which is incorporated herein by reference), and to seize and retain all items listed in Attachment B as instrumentalities and evidence of a crime.

3. The information contained in this affidavit is based on my personal knowledge and experience, my own investigation, and information provided by other law enforcement officers and/or agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause of evidence of violations of 18 U.S.C. § 2252A(a)(1) (transportation of child pornography); § 2252A(a)(2)(A) (receipt of child pornography); and § 2252A(a)(5)(B) (possession of child pornography) are located within the SUBJECT COMPUTER and other digital evidence.

DEFINITIONS

4. The term “computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).

5. The term "Internet" is defined as the worldwide network of computers, a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial internet service provider ("ISP"), which operates a host computer with direct access to the Internet.

6. The term "Web site" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

7. The term "Computer system and related peripherals, and computer media" as used in this affidavit refers to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

10. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

15. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

16. For a number of reasons, the use of computers has become one of the preferred methods of trafficking in, trading, producing, and collecting child pornography and other obscene material. Because the distribution of child pornography is illegal, child pornography is not readily available through legitimate domestic businesses; in contrast, child pornography is widely available via computer from individuals who trade such materials on the Internet. Significantly, an individual can utilize a computer in the privacy of his/her own home or office to locate and interact with other individuals offering or seeking such materials. Moreover, he can do so without revealing his true identity. The use of computers thus provides individuals interested in child pornography or obscenity with a sense of privacy and secrecy. Computers also provide such individuals with a convenient method of storing, organizing, and accessing their collections and information concerning others who collect, trade, or distribute such materials.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

17. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the transportation, receipt and collection of child pornography:

- a. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child pornography.
- b. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- c. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- d. Collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

18. On December 17, 2015, your affiant and FBI Agents Jennifer Mullican and Aaron Covey interviewed Jonathan Pavlik at his residence. Agents identified themselves at the door and Pavlik invited agents into his home for a non-custodial interview. Pavlik resides at 5541 Crosscreek Lane, Apt 2107, Benbrook, Texas, which is located in the Northern District of Texas. Pavlik consented to agents searching the computer in his living room, which is described as a homebuilt desktop computer bearing a label MS-7309.

19. I observed that the homebuilt desktop computer had no significant identifiable markings. The computer contained one hard drive, a Western Digital bearing serial number WCC3F0603640. The words "Product of Thailand" were imprinted on the hard drive's label, indicating that the hard drive was mailed, shipped and/or transported in interstate and foreign commerce.

20. During this interview, Pavlik stated that he has downloaded child pornography videos and images many times. He estimated that he had over 500 images and videos on the computer. He primarily used "Sandboxie" and "TOR" to access child pornography on the dark web.

21. After Pavlik accessed the desktop computer with his password, agents identified over 2,000 files containing either content or file names indicative of child pornography. One file reviewed had the file name of "2013-11-bibigon-5-full.avi."

This file is a video file depicting a nude female child, approximately five years of age, performing oral sex on the erect penis of an adult male. Another file reviewed had the file name of "8 yo little girl get fucked in pussy.wmv." This file is a video file depicting a nude female child, approximately five years of age, being vaginally penetrated by the penis of an adult male. The adult male ejaculates on the prepubescent female. Based on my training and experience, these video files constitute child pornography, as defined in 18 U.S.C. § 2256(8).

22. Pavlik stated that he used multiple additional hard drives and USB devices on his computer and is not sure if they contain child pornography or not. He also was also not sure if the other computers in his residence contain child pornography. Pavlik consented to allow the FBI to search all digital items in his residence; your Affiant is aware that those who collect and download child pornography typically use multiple devices to facilitate and/or store child pornography.

23. Based on the interview, Jonathon Pavlik's admissions, and his consent, your affiant seized the SUBJECT COMPUTER and other digital evidence and secured the devices in an access-controlled, secure area pending further forensic examination. The SUBJECT COMPUTER and other digital evidence was seized within the Northern District of Texas and, at the time of the signing of this warrant, is in the custody of the FBI within the Northern District of Texas at the FBI Field Office located at 1 Justice Way, Dallas, Texas.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

24. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

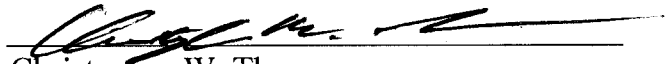
- a. Computer storage devices (like hard disks, magneto opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

25. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s)

may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

CONCLUSION

26. Based on the above information, there is probable cause to believe that the items described in Attachment B are presently located within the SUBJECT COMPUTER and other digital evidence, as set forth in Attachment A and the digital media therein, and that these items constitute evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2)(A), and (a)(5)(B). Accordingly, I respectfully request that the Court authorize the search of the SUBJECT COMPUTER and other digital evidence and the seizure of the evidence and instrumentalities of the above violations of federal law and related contraband.


Christopher W. Thompson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 18, 2015 at 1:50 pm in Fort Worth, Texas.


JEFFREY CURETON
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE ITEMS TO BE SEARCHED

The SUBJECT COMPUTER is described as a homebuilt desktop computer bearing a label MS-7309. The computer contained one hard drive, a Western Digital bearing serial number WCC3F0603640. Other digital evidence to be searched is described as follows:

- Red DT101 G2 8 GB flash drive
- Micro Center 2 GB flash drive
- PNY Technologies Attache 2 GB flash drive
- Dell Laptop computer P/N 7T390 A03
- Three (3) SanDisk SDSSDHII hard drives
- Lenovo ThinkCentre M72e computer, S/N MJXKTVA
- Lenovo ThinkCentre M72e computer, S/N MJ69L1D
- Lenovo ThinkCentre M72e computer, S/N MJ88WR2
- Western Digital 500 GB hard drive, S/N WCC1S6663367
- Western Digital 250 GB hard drive, S/N WCAV2Y404213
- Futitsu 250 GB hard drive S/N K61DT8829JSU

All the devices and the SUBJECT COMPUTER are currently located at the FBI Field Office, at 1 Justice Way, Dallas, Texas.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer hardware, computer drives, computer software, computer passwords, that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
3. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
9. Any and all address books, mailing lists, supplier lists, and any and all documents and records, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).